CLIPPEDIMAGE= JP406284124A
PUB-NO: JP406284124A
DOCUMENT-IDENTIFIER: JP 06284124 A
TITLE: INFORMATION TRANSMISSION SYSTEM
PUBN-DATE: October 7, 1994
INVENTOR-INFORMATION:
NAME
TORIKAI, MASAMICHI
FUJII, MIKIO
INT-CL_(IPC): H04L009/06; H04L009/14 ; G09C001/00
ABSTRACT:

PURPOSE: To assure confidentiality of transmission information by verifying the adequacy of a user terminal equipment relating to information transmission.

CONSTITUTION: A security center means 10 is provided with a means sending a random number key to a satellite means 100 and a means generating and registering a user password of the satellite means 100 by decoding a ciphering key returned from the satellite means 100 at the random key and using a verification key for ciphering processing, and the satellite means 100 is provided with a specific user key and a means generating a ciphering key resulting from ciphering a satellite key based on the provided random number key and returning the generated ciphering key to the security center means 10, or the security center means 10 is provided with a means generating a collation key by decoding the user password with the verification key and ciphering the user password by the random number key and capable of verifying adequacy of the satellite means 100 by collating the ciphering key sent from the satellite means 100 and the collation key.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－284124

(43)公開日　平成6年(1994)10月7日

| (51)Int.Cl.[5] | | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| Ｈ０４Ｌ | 9/06 | | | | | |
| | 9/14 | | | | | |
| Ｇ０９Ｃ | 1/00 | | 8837－5L | | | |
| | | | 8949－5K | Ｈ０４Ｌ | 9/02 | Ｚ |

審査請求　未請求　請求項の数３　ＦＤ　（全　8　頁）

(21)出願番号　特願平5－87877

(22)出願日　平成5年(1993)3月24日

(71)出願人　591234204
株式会社ローレルインテリジェントシステムズ
神奈川県横浜市緑区あざみ野１丁目14番５

(72)発明者　鳥　飼　将　迪
神奈川県横浜市緑区あざみ野１丁目14番５　株式会社ローレルインテリジェントシステムズ内

(72)発明者　藤　井　幹　雄
神奈川県横浜市緑区あざみ野１丁目14番５　株式会社ローレルインテリジェントシステムズ内

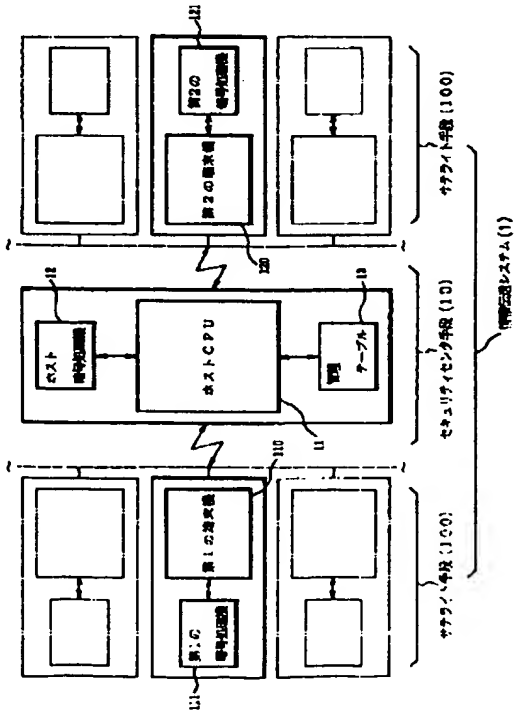
(74)代理人　弁理士　岡田　和喜

(54)【発明の名称】　情報伝送システム

(57)【要約】

【目的】　情報伝送に関するユーザ端末機の正当性を認証することにより伝送情報の機密性を保証する伝送システムの提供。

【構成】　セキュリティセンタ手段においては、サテライト手段に対して乱数キーを送信しうる手段と、サテライト手段から返信された暗号キーを乱数キーにより復号化し、更に認証キーにより暗号化処理することにより、サテライト手段のユーザ暗証を生成し、登録しうる手段とが具備されており、サテライト手段においては、個有のユーザキーを保有しており、セキュリティセンタ手段から提供された乱数キーにより、サテライトキーを暗号化した暗号キーを生成し、これをセキュリティセンタ手段に返信しうる手段を具備し、又セキュリティセンタ手段においては、ユーザ暗証を認証キーにより復号化し、更に、乱数キーにより暗号化することによって、照合キーを生成し、サテライト手段から送信された暗号キーと、当該照合キーとを照合させて、サテライト手段の正当性を認証しうる手段を具備したもの。



1

【特許請求の範囲】

【請求項1】　暗号情報を読出し可能に格納しうるセキュリティセンタ手段と、平文情報を暗号化ならびに復号化処理しうるサテライト手段とを公衆通信回線などにより結線してなる情報伝送システムであって、前記セキュリティセンタ手段においては、前記サテライト手段に対して乱数キーを送信しうる手段と、前記サテライト手段から返信された暗号キーを前記乱数キーにより復号化し、更に認証キーにより暗号化処理することにより前記サテライト手段のユーザ暗証を生成し、登録しうる手段とが具備されており、前記サテライト手段においては、個有のユーザキーを保有しており、前記セキュリティセンタ手段から提供された乱数キーにより、前記サテライトキーを暗号化した暗号キーを生成し、これを前記セキュリティセンタ手段に返信しうる手段を具備してなる情報伝送システム。

【請求項2】　前記セキュリティセンタ手段において、前記ユーザ暗証を認証キーにより復号化し、更に乱数キーにより暗号化することによって照合キーを生成し、サテライト手段から送信された前記暗号キーと、当該照合キーとを照合させて、前記サテライト手段の正当性を認証しうる手段を具備した請求項1記載の情報伝送システム。

【請求項3】　前記セキュリティセンタ手段において、前記サテライト手段のユーザ暗証を認証キーによって復号化し、更に乱数キーによって暗号化してなる暗号化キーを生成する手段と、情報を受領する側のサテライト手段のユーザ暗証を認証キーによって復号化し、乱数キーによって暗号化して復号処理キーを生成する手段とを具備しており、情報を発信する側のサテライト手段においては、前記セキュリティセンタ手段から提供された暗号化キーを、サテライトキーによって復号化して、暗号処理キーを生成する手段と、当該暗号処理キーにより送信する情報を暗号化する手段とを具備しており、更に、情報を受信する側のサテライト手段においては、セキュリティセンタ手段から送信された前記復号化キーをサテライトキーによって復号化して復号処理キーを生成する手段と、前記情報を発信する側のサテライト手段において暗号化された情報を、前記復号処理キーにより復号化処理しうる手段とを具備した請求項2記載の情報伝送システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、公衆電話回線などの通信網を利用した情報伝送技術において、パソコンなどの特定のユーザ端末デバイスの確認および、その特定のユーザ端末デバイスのみによる情報の授受を保障しうる情報伝送システムに関するものである。

【0002】

【従来の技術】従来、機密情報を安全に保管し、又は、

2

伝送するために平文情報を暗号化処理し、パソコンなどの端末デバイスを公衆電話回線によって接続して授受する技術は所謂パソコン通信として広く活用されており、この際、情報伝送の当事者の確認は、例えば、IDコードやパスワードに頼っているのは実状である。

【0003】しかしながら、現実に当該情報にアクセスできる端末デバイス自体の正当性を確認することは、別途電話通信による逆探知手法によるとしても、相当の所要時間を費やすこととなり、実際上は、端末デバイスそのものの正当性を確認することは殆ど不可能であるため、悪意の第三者が、不当に前記のIDコードもしくはパスワードを知得すれば任意の端末デバイスから容易に当該情報を詐取することが可能となるものである。

【0004】このような不安を解消するために、各種の改善提案がなされており、その具体例としては、例えば、特開昭63－155930号公報（公知例）の発明が知られている。

【0005】この公知例のデータ暗号化通信方式は、公衆データ網を利用して、プロトコル変換手段により変換されたデータを、暗号化キーを付加情報としたパケットとして伝送し、保有する復号化手段の特定キーに基づいてデータの復号化を図るようになしたものである。

【0006】

【発明が解決しようとする課題】前記の公知例のものにあっても情報を暗号化して、これを伝送しうるものであるが、その目的とするところは、暗号化手段を保有しないデバイス間で公衆データ網を利用して暗号化データを伝送するものであるから、不特定の第三者によるデータ通信デバイスを用いた暗号化情報へのアクセスはフリーとなり、重要な情報の漏洩を完全に未然防止する点での不安が残るものであり、機密情報の伝送に携わるユーザ側からは、暗号化情報が特定の正当なユーザ間においてのみ授受されることが保障されうるように、そのユーザ端末手段の認証ならびに、認証完了後に暗号化情報が授受される安全な情報伝送装置の提供が切望されるところであった。

【0007】

【課題を解決するための手段】この発明の目的とするところは、暗号ホスト手段と、暗号サテライト手段を公衆電話回線などで結線し、各手段に保有する特有のキーを利用して暗号化もしくは復号化処理を実行し、特定の正当なユーザ端末手段のみが情報にアクセスできるようユーザ認証ならびに情報伝送を可能としたシステムを提供するものであって、その特徴とする点は、次の通りである。

【0008】(1) 暗号情報を読出し可能に格納しうるセキュリティセンタ手段と、平文情報を暗号化ならびに復号化処理しうるサテライト手段とを公衆通信回線などにより結線してなる情報伝送システムであって、前記セキュリティセンタ手段においては、前記サテライト手段に

3

対して乱数キーを送信しうる手段と、前記サテライト手段から返信された暗号キーを前記乱数キーにより復号化し、更に認証キーにより暗号化処理することにより、前記サテライト手段のユーザ暗証を生成し、登録しうる手段とが具備されており、前記サテライト手段においては、個有のユーザキーを保有しており、前記セキュリティセンタ手段から提供された乱数キーにより、前記サテライトキーを暗号化した暗号キーを生成し、これを前記セキュリティセンタ手段に返信しうる手段を具備してなる情報伝送システム。

【０００９】(2) 前記セキュリティセンタ手段において、前記ユーザ暗証を認証キーにより復号化し、更に乱数キーにより暗号化することによって照合キーを生成し、サテライト手段から送信された前記暗号キーと、当該照合キーとを照合させて、前記サテライト手段の正当性を認証しうる手段を具備した前記(1) 記載の情報伝送システム。

【００１０】(3) 前記セキュリティセンタ手段において、前記サテライト手段のユーザ暗証を認証キーによって復号化し、更に乱数キーによって暗号化してなる暗号化キーを生成する手段と、情報を受領する側のサテライト手段のユーザ暗証を認証キーによって復号化し、乱数キーによって暗号化して復号処理キーを生成する手段とを具備しており、情報を発信する側のサテライト手段においては、前記セキュリティセンタ手段から提供された暗号化キーを、サテライトキーによって復号化して、暗号処理キーを生成する手段と、当該暗号処理キーにより送信する情報を暗号化する手段とを具備しており、更に、情報を受信する側のサテライト手段においては、セキュリティセンタ手段から送信された前記復号化キーをサテライトキーによって復号化して復号処理キーを生成する手段と、前記情報を発信する側のサテライト手段において暗号化された情報を、前記復号処理キーにより復号化処理しうる手段とを具備した前記(2) 記載の情報伝送システム。

【００１１】

【作　　用】この発明の構成は、以上の通りであるから、サテライト手段からの要請によりセキュリティセンタ手段において乱数キーを送信し、サテライト手段において、この乱数により個有のサテライトキーを暗号化してセキュリティセンタ手段に返信し、セキュリティセンタ手段において乱数キーにより一旦これを復号化し、更に認証キーによってこれを暗号化してユーザ暗証を登録＊

4

＊し、又、情報伝送の際には、乱数キーを受信したサテライト手段により、前記暗号化した暗号キーをセキュリティセンタ手段において、照合キーと照合させてサテライト手段のユーザ端末機を認証するものである。

【００１２】次で、情報の伝送の際にも、セキュリティセンタ手段において、同様に復号・暗号化処理を実行して暗号化キーと復号化キーを生成し、情報発信側のサテライト手段では、暗号処理キーを生成し、このキーにより情報を暗号化し、情報受信側のサテライト手段においては、復号処理キーを生成し、このキーにより情報を復号化するものである。

【００１３】

【実　施　例】次に、この発明の実施例を図面に基づいて説明する。図１には、この実施例の情報伝送システム（１）に関する機能ブロック図が示されており、当該システム（１）を構成するセキュリティセンタ手段（１０）は、公衆電話回線、ＬＡＮあるいはＩＳＤＮ回線などの公衆通信網を利用して、多数のサテライト手段（１００）と接続されたものである。

【００１４】又、前記セキュリティセンタ手段（１０）は、ホストＣＰＵ（１１）にホスト暗号処理機（１２）および管理テーブル（１３）が接続された構成とされており、その機能としては、特定ユーザ端末機の認証ならびに当該端末機との暗号情報の授受を可能とするものであるが、その詳細は後述する。

【００１５】又、前記サテライト手段（１００）は、第１，第２……の端末機（１１０），（１２０）……と、各端末機（１１０），（１２０）……に接続された第１，第２……の暗号処理機（１１１），（１２１）……によって構成されており、その機能としては、特定のユーザ端末機の登録ならびに暗号情報の授受を可能としたものであるが、その詳細についても後述する。

【００１６】次に、この実施例のシステム（１）による特定ユーザ端末機の登録・確認ならびに暗号情報の授受について、例えば、同一企業内における財務部と営業部との間で重要な財務情報を授受する場合を想定してその内容を説明する。

【００１７】なお、この出願明細書等における情報の暗号化ならびに復号化に関する数式は、式１によるものと定義する。

【００１８】

【数１】

$$K0 = E_Z\ [D_Y\ (X)\ ] \quad \cdots\cdots\cdots\cdots\cdots\cdots 式1$$

【００１９】即ち、この式１の内容は、情報（Ｘ）を暗号キー（Ｙ）により復号化（デサイファー）し、更に、暗号キー（Ｚ）により暗号化（エンサイファー）した結果は、函数出力（Ｋ０）としてとらえられることを意味するものである。

【００２０】①　特定ユーザ端末機の登録

※先ず、財務部と営業部との間の情報の授受に先立って、両部門に設置されたユーザ端末機をそれぞれ第１の端末機（１１０），第２の端末機（１２０）と仮定し、これらを予めユーザ登録しなければならない。この登録の手順を、図２に示すフローチャートをも参照して説明すると、次の通りである。